Claims

What is claimed is:

1. A system for monitoring data transferred via an FTP protocol comprising:

a client;

a server operating as an intermediary between said client and a foreign network;

an audit database; and

an audit module comprising:

logic for monitoring said data transferred via FTP protocol; and

logic for recording at least a portion of said data transferred via FTP protocol to said audit database.

2. The system of claim 1 wherein said client is capable of receiving data from said foreign network.

3. The system of claim 2 wherein said logic for monitoring operates to monitor data that said client receives from said foreign network.

4. The system of claim 3 wherein said audit module further comprises:

logic for recording metadata associated with said data that said client receives from said foreign network and wherein said logic for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network.

5. The system of claim 3 wherein said logic for recording operates to record all data that said client receives from said foreign network.

6. The system of claim 3 wherein said audit module further comprises:

logic for recording metadata associated with said data that said client receives from said foreign network.

7. The system of claim 4 wherein said logic for recording all data operates to record said data only if said logic for monitoring said data transferred via FTP protocol determines that said data that said client receives from said foreign network comprises at least one of:

pornographic data;

image data;

audio data; and

terrorist activity data.

8. The system of claim 5 wherein said audit module further comprises company guidelines defining acceptable content wherein said logic for recording all data operates to record said data only if said audit module determines that said data that said client receives from said foreign network is in violation of said company guidelines.

9. The system of claim 1 wherein said client is capable of transferring data to said foreign network.

10. The system of claim 9 wherein said logic for monitoring operates to monitor data that said client transfers to said foreign network

11. The system of claim 9 wherein said logic for recording data operates to record all data that said client transfers to said foreign network.

12. The system of claim 11 wherein said audit module further comprises:

logic for recording metadata associated with said data that said client transfers to said foreign network.

13. The system of claim 10 wherein said audit module further comprises:

logic for recording metadata associated with said data that said client transfers to said foreign network and wherein said logic for recording at least a portion operates to record all data that said client transfers to said foreign network.

14. The system of claim 13 wherein said logic for recording all data that said client transfers to said foreign network operates to record said data only if said logic for monitoring said data transferred via FTP protocol determines that said data that said client transferred to said foreign network comprises at least one of:

proprietary company information;

confidential company information;

pornographic data;

image data;

audio data; and

terrorist activity data.

15. The system of claim 11 wherein said audit module further comprises company guidelines defining acceptable content wherein said logic for recording all data that said client transfers to said foreign network operates to record said data only if said audit module determines that said data that said client transferred to said foreign network is in violation of said company guidelines.

16. The system of claim 1 wherein said audit database comprises:

a table structure organized to comprise:

a field to store data related to a client who originated a transfer of said data;

a field to store data related to a destination of said transferred data;

a field to store data related to a name of said transferred data;

a field to store data related to a date that said data was transferred;

a field to store data related to a size of said transferred data; and

a field to store said transferred data.

17 The system of claim 1 wherein said client is an employee workstation connected to an employer's local area network.

18. The system of claim 2 wherein said audit module and said audit database are part of said intermediary server.

19. The system of claim 2 wherein said audit module is part of said intermediary server.

20 A method for transparently auditing FTP traffic comprising:

defining a first computer to act as an intermediary between a second computer and a third computer;

defining an audit database; and

defining an audit module comprising:

logic for monitoring data transferred via an FTP protocol.

21. The method of claim 20 further comprising:

disposing said audit module in said first computer.

22. The method of claim 20 further comprising:

recording said data transferred via an FTP protocol to said audit database.

23. The method of claim 22 further comprising:

recording metadata associated with said data transferred via an FTP protocol to said audit database.

24. The method of claim 20 wherein said logic for monitoring data transferred via an FTP protocol comprises:

monitoring an FTP control port of a computer receiving said data transferred via an FTP protocol;

monitoring an FTP data port of said computer receiving said data transferred via an FTP protocol; and

recording said data transferred via an FTP protocol to said audit database when said logic for monitoring said FTP data port determines that a request to transfer data via said FTP data port has occurred.

25. The method of claim 22 wherein said second computer is located in a intranet and said third computer is located in a network that is foreign to said intranet.

26. The method of claim 25 wherein said data transferred via an FTP protocol is recorded to said audit database upon a finding of either one of:

said second computer connecting to said third computer and said second computer sending data from said second computer to said third computer; and

said second computer connecting to said third computer and said second computer receiving data sent from said third computer to said second computer.

27. The method of claim 26 wherein said data received from said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said received data comprises at least one of:

pornographic data;

image data;

audio data; and

terrorist activity data.

28. The method of claim 26 further comprising:

defining company guidelines that define acceptable content wherein said data received from said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said received data is in violation of said company guidelines.

29. The method of claim 26 wherein said data sent from said second computer to said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said transferred data comprises at least one of:

proprietary company information;

confidential company information;

pornographic data;

image data;

audio data; and

terrorist activity data.

30. A mechanism for auditing data transferred via FTP comprising:

a means for transparently monitoring said data transferred via FTP; and

a means for recording at least a portion of said data transferred via FTP.

31. The mechanism of claim 30 further comprising:

a means for recording metadata associated with said data transferred via FTP.

32. The mechanism of claim 31 wherein said means for recording further comprises a means for organizing said data transferred via FTP.

33. A computer program product having a computer readable medium having computer program logic recorded thereon for monitoring data transferred via an FTP protocol, the computer program product comprising:

code for transparently examining data transferred via an FTP protocol; and

code for recording at least a portion of said data transferred via an FTP protocol.

34. The computer program product of claim 33 wherein said code for transparently examining comprises:

code for determining an origination point of said data transferred via an FTP protocol; and

code for determining an end point of said data transferred via an FTP protocol.

35. The computer program product of claim 34 wherein said code for transparently examining further comprises:

code for determining a filename of said data transferred via an FTP protocol;

code for determining a date said data transferred via an FTP protocol was transferred; and

code for determining a filesize of said data transferred via an FTP protocol.

36. The computer program product of claim 34 wherein said code for recording comprises:

code for recording said data transferred via an FTP protocol; and

code for recording metadata associated with said data transferred via an FTP protocol.

37. The computer program product of claim 36 wherein said code for transparently examining data further comprises:

code for determining if said data transferred via an FTP protocol is suspicious wherein said data transferred via an FTP protocol is suspicious if said data transferred via an FTP protocol comprises at least one of:

proprietary company information;

confidential company information,

pornographic data;

image data;

audio data; and

terrorist activity data.

38. The computer program product of claim 36 wherein said code for transparently examining further comprises:

code defining company guidelines that define acceptable content; and

code for determining if said data transferred via an FTP protocol is in violation of said company guidelines.

39. The computer program product of claim 38 wherein said code for recording data transferred via an FTP protocol executes to record said data transferred via an FTP protocol only if said code for transparently examining determines that said data transferred via an FTP protocol is in violation of company guidelines.

40. The computer program product of claim 37 wherein said code for recording said data transferred via an FTP protocol will record said data transferred via an FTP protocol only if said data transferred via an FTP protocol is suspicious.